Colleges and universities are prime cyber attack targets

March 10, 2016

A recent cyber attack at the University of California, Berkeley is just one of many recent security threats on higher education institutions. The attack on the university's computer system, which occurred in late December, jeopardized the financial data of more than 80,000 people, including students, faculty, alumni and vendors. Similar hacking attempts at colleges and universities are becoming increasingly frequent, often occurring on a daily basis and unbeknownst to the institution. Universities are increasingly vulnerable to cyber attacks, which can be costly. However, there are a few tips in dealing with cyber events that every higher education administrator should know.

Why universities are vulnerable

Colleges and universities maintain large stores of sensitive data, including financial information and expensive research statistics, making them prime targets for hackers around the world. In addition, universities are often unable to adequately defend against hacking attempts due to budgetary constraints and understaffing. As a result, universities are increasingly vulnerable to hackers, who may have previously focused on large corporations.

In 2014, 10 percent of reported security breaches involved the education sector, according to Symantec's Internet Security Threat Report. Only the health care and retail sectors experienced more security breaches than the education sector. In 2015, 550 universities reported some kind of data breach. Of these universities, institutions of all sizes have been targeted — from Pennsylvania State University, whose engineering department system was breached in 2015, potentially affecting 18,000 student and faculty, to the Maricopa County Community College District in Arizona, which possibly affected more than two million students.

Why the attacks are costly

Cyber attacks can be costly for universities. According to the Ponemon Institute, the education sector has one of the highest per capita data breach costs at $259 for each record containing sensitive information. In addition, depending on the severity of a breach, it is likely that a university will find itself defending an expensive lawsuit. For example, the Maricopa breach resulted in two class-action lawsuits that, combined, cost the college $2.3 million to settle.

Dealing with an attack

To avoid the significant consequences that can result from a cyberattack, colleges and universities should take affirmative steps to strengthen their networks and protect their personal information. Though colleges and universities face unique difficulties in defending against cyberattacks, there are ways to prepare when a hacking attempt occurs, which is becoming more and more inevitable.

1. Be cognizant of the threat of cyber attacks. It is not a matter of if a cyber attack will occur; it is a matter of when. Just like businesses, colleges and universities would do well to have a cybersecurity plan in place — both to strengthen current cybersecurity measures and have a plan for when an attack does occur.
2. Look outside your organization for help in strengthening your network and computer system. This may include a private company or even the Federal Bureau of Investigation (FBI), which has programs designed to assist universities on

safeguarding data.

3. If your budget is limited, prioritize the most sensitive information. Expend the funds to protect the most sensitive or important information.
4. Consider cyber insurance, which can include helpful services such as privacy breach notifications, computer fraud protection, and cyber incident preparation and response plans.

Authors